International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Rethinking Consideration in the Digital Economy: Can User Data Constitute Valid Consideration Under Indian Contract Law?

Dhayal Sivachidambaram

II Year BBA., LLB., (Hons.), Sastra Deemed to be University, Thanjavur, Tamil Nadu

ABSTRACT

This study investigates whether online attention and personal information can be considered legitimate consideration under Indian contract law. According to the conventional theory (Section 2(d) of the Indian Contract Act), a promise must be accompanied by "something done or promised"[1]. Many services in the digital economy seem "free," but users really pay with their attention and important personal information [2]. In order to find gaps and difficulties, this study examines the policy environment, contemporary practices[3], and historical underpinnings of the law. To determine whether data can be considered an exchange, we examine Section 2(d) and related rules (such as Sections 10 and 23) in conjunction with data-privacy principles (most notably Puttaswamy's privacy finding). To frame the discussion, instances (such as Google, Facebook, and WhatsApp) and international studies are examined. The results imply that the broad definition of consideration in Indian law. but privacy rights and unequal bargaining power impose practical limits. We conclude by recommending clearer legal recognition of data-for-service contracts and stronger consumer safeguards in digital agreements.

Keywords: Consideration, Personal information , Digital agreements

INTRODUCTION

A "give-and-take" has always been necessary for contracts. According to Section 10 of the Indian Contract Act, 1872, an agreement is only enforceable if it is made with "free consent... by parties competent to contract, for a lawful consideration and with a lawful object"[4]. Traditionally, consideration refers to the exchange of products, services, or money. However, new types of value exchange have been introduced by contemporary markets, particularly online platforms. Mobile apps, social media, and search engines are frequently provided "free of charge," but user attention and personal data are the hidden costs. This

[1] Section 2 in The Indian Contract Act, 1872
https://indiankanoon.org/doc/831280/
[2] Personal Data as Consideration
https://ejournals.eu/pliki_artykulu_czasopisma/pelny_tekst/018e9e53-aada-73b1-8423-be6c10bfc41e/pobierz
[3] India's internet users to exceed 900 million in 2025, driven by Indic languages | IBEF
https://www.ibef.org/news/india-s-internet-users-to-exceed-900-million-in-2025-driven-by-indic-languages
[4] The Indian Contract Act, 1872
https://indiankanoon.org/doc/171398/

change begs the fundamental question: Can digital activity and personal data be taken into account under Indian law?

HISTORICAL BACKGROUND

The Indian Contract Act of 1872 contained colonial common law ideas that are the source of the Indian legal concept of consideration. "Something done, or abstained from doing, or promised to be done or abstained from, at the desire of the promisor" is what Section 2(d) defines as consideration. Indian courts have given this a wide interpretation. Chinnaya v. Ramayya (1882), for instance, confirmed that consideration may come from any person, not just the promisee. The Act does not stipulate that consideration must be sufficient or monetary. Therefore, a pledge supported by a modest or even nominal conduct may nevertheless be enforceable. In the past, this theory distinguished contracts from simple social commitments by guaranteeing that only agreements involving reciprocal trades were upheld. Contracts devoid of consideration, such as promises of gifts, are typically null and void.

Indian courts have further stressed that any deed or forbearance asked by the promisor qualifies as compensation; money is not necessary. For instance, it has been decided that abstaining from an action (like giving up a right) constitutes legitimate thought. This ambiguous interpretation implies that "give-and-take" in whatever form is acceptable under the law. Section 23, which states that consideration (or object) must be legal and not contrary to public policy, is the only explicit restriction [5].

CURRENT SCENARIO

Major firms provide services (social networks, email, search, etc.) "for free" in the current digital economy. However, these platforms use algorithmic profiling and targeted advertising to commercialize the precise personal data they gather (search history, location, biometrics) .Users essentially "pay" with data. India has seen a tremendous increase in internet usage; by 2025, there will be more than 900 million active users. Digital services have become a part of everyday life due to smart devices and more affordable data. Each click, like, and view produces data that can be sold. Businesses use the "attention economy" to monetize attention to such an extent that human focus itself becomes a commodity. Scholars of surveillance-capitalism observe that human actions have substantial economic worth when they are analyzed by algorithms.

Users rarely view this transaction as a "contract," nevertheless. Unaware that they are handing up important information, they can click "I agree" to a privacy policy without reading it. Customers have less negotiating leverage because digital transactions are standardized (clickwrap/shrinkwrap) and non-negotiable. In light of this, established contract principles—which were created for tangible goods—are under pressure. The question of whether exchanging data can satisfy the requirement of consideration is still unclear in Indian law.

KEY ISSUES AND CHALLENGES

Consent and information privacy are major concerns. Contracts with illegal or public policy-opposing objects are null and void under Section 23. Contracts that commodify personal data may violate privacy

[5] Data as Consideration: Re-examining the Concept of Value under Modern Contract Law - The Lawscape https://www.thelawscape.in/personal-data-as-legal-consideration-indian-contract-law/

standards if it is intrinsically private (a fundamental right according to Puttaswamy)[6]. Agreements that grant broad data rights without informed permission may be difficult for courts to sustain. According to one author, "Courts may set aside agreements under Section 23 when they attempt to claim wide or endless rights to use someone's data". Therefore, even in cases when consideration is technically present, concerns about fairness and free consent are significant.

Information asymmetry presents another difficulty. Platforms know exactly how they earn from data, but users do not. Consumers rarely grasp the economic value of what they give away. This creates a bargaining asymmetry. The Lawscape report pointed out that "most online agreements come with fixed rules… Since humans cannot bargain, the assumption that contracts reflect fair conversation breaks out when one side retains all the control" .Consumer protection principles may intervene, but remedies for data-driven harms are weak.

Furthermore, the valuation of data is abstract. Unlike money, data has no fixed price tag. It can be copied and reused indefinitely. Courts may struggle to quantify loss if, say, data is misused. As one scholar remarks, "not like a chair or a phone, data doesn't come with a set price tag… data harms don't fit old molds". This evidentiary difficulty complicates enforcing any implied quid-pro-quo. In sum, while consideration's presence may be arguable, its lawfulness and fairness depend on how privacy and consent are managed.

FACTORS INFLUENCING THE SITUATION

Several factors shape this landscape. Technology and business models play a big role: advances in AI and cloud computing have made personal data extremely lucrative, entrenching business models that trade in "free" services for data. Market structure matters too: few large digital platforms (often with monopolistic traits) control most online services, reducing users' choices. This concentration influences contract power.

On the legal side, India's recognition of privacy as a fundamental right (in Puttaswamy v. Union of India 2017) is transformative[7]. The Supreme Court held that privacy (including data privacy) is protected under Article 21, meaning that individuals have autonomy over personal information. This doctrinal shift emphasizes individual dignity and may limit contracts that unduly invade privacy.

Cultural and behavioral factors also influence consent. Many Indian users readily share some information (e.g. religious or caste identifiers) on social media, but consider financial or medical data more sensitive. The rapid digitalization of rural India (55% of internet users were rural in 2024) is closing the access gap, but awareness of data risks remains uneven. Events like WhatsApp's controversial 2021 privacy update (which required users to share metadata with Facebook or exit the app) exposed public sensitivities[8]. When that change was announced, mass outcry and regulatory pressure forced WhatsApp to delay implementation. This incident highlighted the power of big tech (they can impose terms "take it or leave it") and the limits imposed by public scrutiny and government action.

[6] Privacy As A Fundamental Right:Impact And Implementation After Puttaswamy
https://www.ijllr.com/post/privacy-as-a-fundamental-right-impact-and-implementation-after-puttaswamy

[7] Privacy As A Fundamental Right:Impact And Implementation After Puttaswamy
https://www.ijllr.com/post/privacy-as-a-fundamental-right-impact-and-implementation-after-puttaswamy

[8] The Privacy Conundrum: An Empirical Examination of Barriers to Privacy Among Indian Social Media Users – The Philosophy and Law of Information Regulation in India
https://publications.clpr.org.in/the-philosophy-and-law-of-information-regulation-in-india/chapter/1/

GOVERNMENT AND POLICY RESPONSES

India has started to close legislative loopholes in response to privacy and data concerns. The government started a data protection framework after Puttaswamy. Based on the Srikrishna Committee, the Personal Data Protection Bill (2019) would have created extensive guidelines for handling personal data. The Digital Personal Data Protection Act of 2023 was made possible by the bill, notwithstanding its expiration. The DPDP Act was passed in August 2023 and will begin to take effect gradually in late 2025[9]. It requires consent before processing personal data and gives people rights (to information, correction, and erasure). In essence, it acknowledges that personal information is valuable and ought to be managed legally.

Regarding contracts, e-contracts are already covered by India's Information Technology Act 2000. Digital signatures are legally valid under Section 5 of the IT Act, and contracts created electronically cannot be declared invalid only because they are digital, according to Section 10A[10]. Therefore, in theory, electronic agreements are accepted by the law (meeting offer, acceptance, consideration). However, privacy protections were initially absent from the IT Act; the DPDP Act now fills that gap.

The proposed Non-Personal Data (NPD) framework, which aims to consider some anonymised data as a communal resource, is one of the other policy initiatives. In accordance with antitrust rules, the Competition Commission of India has also begun to examine data practices (e.g., a 2023 case against Big Tech for unfair data use). Unfair terms are now recognized by consumer protection regulations in digital contracts. In sum, policy responses are emerging to acknowledge both data's value and the need for individual rights, but legislation specifically treating data as contractual consideration remains lacking.

OBJECTIVE OF THE STUDY

This study's main goals are:

- To determine if user attention, personal information, and other digital inputs can be considered legitimate "consideration" under the Indian Contract Act of 1872.
- To assess how well contemporary, intangible forms of commerce are accommodated by the notion of consideration in Section 2(d).
- To find legal gaps, such as those between contract law and data privacy standards, and the realities of the digital economy.
- To examine international and comparative viewpoints on data as contractual value, with an eye toward India.
- To make policy and legal suggestions for managing data-driven exchanges, such as consumer protections and statutory reforms.

These goals will direct the analysis and guarantee that every part tackles a facet of the main research subject.

LITERATURE REVIEW

In order to determine the research gap, this part examines the body of work that has been done on data, contracts, and consideration both domestically and abroad.

[9] The Digital Personal Data Protection Bill, 2023
https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023

Classical Contract Doctrine: According to traditional literature, consideration must be something of value and is defined as "the price for which the promise of another is bought". There is scant treatment of intangible or informational value in standard contract law literature (e.g., Pollock & Mulla on Contract, Chitty on Contracts), which concentrates on tangible commodities or services. Indian commentary, such as domestic law comments, also highlights the need for consideration to be both lawful and move at the promisor's request. These sources, however, frequently predate digital markets and do not specifically take data or attention into account.

New Research on Data and Contracts: Researchers have started looking into "data as consideration" in recent years. Personal data may have commercial worth and "function as a consideration" in contracts, according to a prominent European investigation by Dudás et al.. They argue that as the GDPR regime does not expressly prohibit treating data as payment, the European Data Protection Board (EDPB) should not automatically invalidate data exchanges as anti-privacy. Indeed, the asset-like nature of data is tacitly acknowledged by EU legal initiatives such as the Data Act and Data Governance Act. However, these point out that the legal question of whether or not one can pay for a service with data remains unresolved, leaving it up to the courts to decide. This raises the question of whether contract law should change on a worldwide scale.

US and EU Perspectives: Some have advocated for updating consideration in common law jurisdictions. Articles on Cornell law, such as "Rethinking Consideration in the Electronic Age" by Merry J. O'Connor, examine how traditional doctrines are challenged by digital services. For instance, they note that consent to data use is frequently included in online contracts rather than money, which begs the question of whether consent to data collecting qualifies as "consideration." These studies highlight similarities between data and more conventional "non-monetary" factors, such as pledges to forgo a legal right [11].Researchers also contrast California's CCPA with GDPR, arguing that although the CCPA at least acknowledges customers' rights to opt out of data sales, GDPR prohibits processing personal data based on data-subject considerations. These comparative pieces underline that some jurisdictions implicitly acknowledge data's value, while others remain cautious.

Digital Contracts in India: The literature on contracts and data value is scarce in India. The majority concentrate on consumer protection and the enforceability of digital contracts. For example, Sharma (2022) looks at Sections 5 and 10A of the IT Act, which acknowledge e-contracts[12]. He points out that electronic agreements that meet the requirements of offer, acceptance, and consideration are specifically upheld by Section 10A. However, academics note that there are no particular data-privacy protections in the IT Act. By requiring legitimate consent and processing, the DPDP Act (2023) closes that gap. However, the way that current contract law handles the actual data transmission has not yet been thoroughly examined in legal commentary.

Contract vs. Privacy Literature: Several studies look at how contract law and data protection interact. For instance, Pirzada (2024) talks about how standard form "clickwrap" agreements frequently compromise genuine consent. Given the basic right to privacy, she proposes that Indian courts may examine such

[11] Personal Data as Consideration
https://ejournals.eu/pliki_artykulu_czasopisma/pelny_tekst/018e9e53-aada-73b1-8423-be6c10bfc41e/pobierz

[12] Signing the Future: How E-Contracts Are Redefining Global and Indian Contract Law.
https://www.vintagelegalvl.com/post/signing-the-future-how-e-contracts-are-redefining-global-and-indian-contract-law

agreements for free consent under Sections 13–14 of the Contract Act. Another argument points out that contracts that compromise privacy may be void due to Section 23's public policy limb. According to Choudhary (2023), data-for-service contracts may be unethical due to data subjects' lack of bargaining power. These works draw attention to conflicts: privacy law requires that people maintain control over their information, whereas contract law permits any compromise[13].

Empirical and Policy Studies: Non-legal studies (such as IAMAI reports) verify that Indians are using social media and applications more often, frequently without taking privacy settings into account. According to a CLPR survey, many Indians prioritize financial data over the privacy of demographic information. Policy analyses (Think Tank briefs, PRS and ICRIER publications) highlight the government's initiatives (Privacy Bill, DPDP Act) and digital infrastructure while discussing India's data economy in general. But rather than discussing the contractual status of data exchanges, these sources focus primarily on privacy protection.

Gap in the Literature: Although data protection and privacy rights have been extensively researched, there is a dearth of legal scholarship that specifically examines whether data can be treated as consideration under Indian contract law. Previous research has either concentrated on privacy as a fundamental right or on e-contract formalities. None specifically examine Section 2(d) in relation to transactions involving user data. By combining contract theory, privacy law, and the realities of the digital economy, this study seeks to close that gap.

CONCEPTUAL FRAMEWORK

This section develops the theoretical model of “data-for-service” contracts, supported by examples and international comparisons.

DATA AS INTANGIBLE CONSIDERATION

According to the classical concept, adequacy is unimportant because consideration just needs to exist in some form. Non-monetary transfers are upheld as consideration in common law examples (e.g., withholding from a right was upheld in Hamer v. Sidway). According to this reasoning, disclosing personal information is a "act done at the desire of the promisor" , and as such, it is first covered by Section 2(d). Intangible acts, such as a marriage contract, have long been recognized as consideration by Indian courts. Consequently, one could contend that consenting to monitoring or freely supplying data constitutes a "something" provided in exchange for the service. This flexibility is emphasized in the Lawscape analysis: "Even if nothing physical changes hands, the rules stretch easily to include such invisible exchanges".

Nonetheless, a number of doctrinal issues come up: First, is data sufficiently "valuable"? Courts may accept even negligible value since they typically do not evaluate adequate thought. However, customers' data is obviously valuable if they bring in billions of dollars from advertisements. Second, consent is ambiguous: Section 14 mandates that it be free from force or deception, whereas Section 13 demands consent. Is user consent genuinely informed if they click away long terms? Contract law does not necessitate extensive "bargaining," but it does call for consensus. Many clickwrap agreements, according to critics, create a "consent gap" because users aren't negotiating on an equal basis.

[13] Data as Consideration: Re-examining the Concept of Value under Modern Contract Law - The Lawscape https://www.thelawscape.in/personal-data-as-legal-consideration-indian-contract-law/

In the past, the GDPR regime avoided defining data as consideration, emphasizing permission and legitimate interest as distinct concepts. According to the European Data Protection Board, in order to prevent problems with privacy rights, personal data should not be seen as payment.According to Dudás et al. (2023), this position may cause issues since it prevents judges from evaluating possible effects. Crucially, their study reveals that paying with data is not expressly prohibited by EU law, leaving courts to determine whether and when the transfer of personal data qualifies as consideration.

CASE STUDIES AND EXAMPLES

- Social Media (Meta/Facebook): Facebook offers social networking for free. Users agree to comprehensive data collecting and tracking (likes, interests, location) in return. The majority of Meta's revenue comes from the sale of targeted advertisements. Users' data sharing may be the consideration if it were presented as a contract. Many consumers, however, don't expressly consent to a charge; instead, their unpaid "consent" is buried in the language. A court might consider every post or "like" as part of a quid-pro-quo if users had negotiated.
- Search engines: Google Search is free, but each hit and query is recorded. Although Google's use of that data (to improve services and advertisements) is obviously transactional, their "consent" is concealed in policies. One could analogize a case where a customer agrees to buy a product at a discount if they consent to marketing emails. Here, data replaces money.
- Streaming and Apps (YouTube, TikTok, etc.): Users' attention and data are "charged" by free video streaming services like YouTube. As a local example, TikTok uses an algorithm based on user behavior. Governments take the value of user data very seriously, as evidenced by the recent TikTok ban difficulties in India (data security worries).
- Online marketplaces (Amazon, Uber): In exchange for purchase history, preferences, and ratings, even e-commerce sites offer "free" basic app access. Aside from delivery costs, personal information influences future tailored pricing or suggestions.

Hidden contracts are demonstrated by these cases. They are in a gray area legally; Indian courts have not yet decided any cases stating that "your data was the consideration," yet there are similarities. In a standard service contract, for example, one party may give authority to conduct X as payment. It is challenging to demonstrate a true contract (offer, acceptance, or meeting of minds) in these situations. However, the fundamental trade—data for service—is indisputable.

INTERNATIONAL SCENARIO AND COMPARISON

Similar problems are being faced by a number of jurisdictions worldwide. As said, the EDPB's 2019 guidelines in the EU suggested that processing personal data should not be justified as a contract consideration (to prevent compromising privacy). However, data-sharing is acknowledged as an economic activity under the future EU Data Act (2022) and Data Governance Act (2022), but primarily in the context of business-to-business transactions. The European attitude is changing. For instance, the EU's 2019 Digital Content Directive recognizes that digital content may be supplied in exchange for "non-monetary consideration," but it leaves specifics up to member states.

Customers in the US have the option to refuse data sales under the California Consumer Privacy Act (CCPA), which also imposes criminal penalties for unapproved data sales. Given that the CCPA treats the sale of data similarly to the sale of products, this suggests that the market worth of the data is acknowledged. However, data as a contractual quid pro quo has not been clearly handled by U.S. contract

law (such as New York's UCC). According to some American academics, if parties genuinely consent, common law, which supports contract freedom, would probably permit personal data as consideration.
Few developing countries outside of the West have addressed this doctrinally. Although it must take into account local beliefs, India's treatment will probably be based on international norms. India's contract law "already allows many forms of value – as long as laws are followed – making space for personal information to count," according to the Lawscape article[14]. Section 2(d) is, in fact, neutral toward technology. The emphasis on autonomy in Western contracts may not align with other Indian legal traditions, such as some consumer protection standards. For instance, unreasonable standard terms may be void under consumer law.
In conclusion, there is no worldwide agreement: some legal systems rely on privacy rules to restrict data payments, while others implicitly allow them (at least indirectly). This uncertainty is a component of the research gap; we need to use this comparative perspective to analyze Indian law's position.

SOLUTIONS AND RECOMMENDATIONS

Given the analysis above, several solutions emerge:

- Statutory Recognition of Data Consideration: If personal information is freely provided, the Indian Contract Act may be changed or judicially interpreted to expressly acknowledge it as a legitimate form of consideration. If the promisor requests it, a clarification (possibly in Section 2(d) explanations) could specify that "acts involving transfer or use of personal data" constitute as consideration. By doing this, unnecessary confusion would be avoided and the law would be in line with reality.
- Enhanced Consent Standards: When data is transferred for services, legislation or regulation should mandate explicit, detailed consent in order to close the consent gap. For instance, contracts including personal data should be presented in an intelligible way according to data protection laws (such as the DPDP Act). Digital literacy efforts can complement this. Ensuring that consent to data use is truly informed will bolster the enforceability of such contracts.
- Integration of Contract and Privacy Law: In data cases, courts ought to implement Section 23 more clearly. Contracts that guarantee improper data releases ought to be declared null and unenforceable because they violate public policy. However, a balanced approach is required instead of outright prohibitions. Guidelines on acceptable data-for-service agreements (similar to prohibiting exploitative clauses) could be issued by regulators. The goal is to preserve dignity without making all data contracts void.
- Unfair Terms Review: Platform agreements should be closely examined by consumer protection organizations, such as the Competition Commission or consumer courts. A clause may be overturned if it unjustly denies consumers their basic data rights (without a fair trade). Under consumer law, the idea of unconscionability might also be useful. Promoting dispute resolution procedures for digital contracts can help users who feel deceived.
- Data Valuation Transparency: Lawmakers may mandate or encourage businesses to reveal how user data is monetized. An "info economy" index or an annual report measure might be used to demonstrate this transparency. Users can make better selections if they are aware of the financial worth of their data. Technologically, instruments (such as data wallets) could be created to monitor the transfer of personal data.

[14] https://www.thelawscape.in/personal-data-as-legal-consideration-indian-contract-law/

- Judicial Guidelines: For instances involving digital exchanges, courts may create doctrines. For instance, courts may modify established standards of unjust enrichment or defamation when determining compensation for unapproved data usage. Contractual remedies may be supplemented by new remedies, such as statutory damages for data breaches. Legal innovation may be sparked by the Lawscape article's suggestion of "flexible ways to show what happened, since data harms don't fit old molds".

The main goals of the recommendations are to safeguard people and make the law more clear. The objective is to guarantee fair trade and respect for rights, not to stop data-driven services.

FUTURE PROSPECTS

The importance of taking data into account will only increase. The need for user data will rise as personalized services and artificial intelligence become more widespread. Globally, legal systems are changing to take this into account. The DPDP Act and upcoming regulations (which will go into effect in 2025) would establish fundamental privacy rights in India. It needs to be seen if these develop to specifically handle contract considerations.

It is conceivable that lawsuits involving data sharing would come before Indian courts. If a customer sues an app for not providing promised services after data is acquired[15], or if a data breach raises concerns about contract obligation, future jurisprudence might develop. As it did with arbitration clauses and internet offenses, the judiciary may modify current standards.

In terms of legislation, India might take into consideration a specific law or amendment that focuses on e-commerce contracts and may be affected by global models. The ability to enforce these measures will determine their success. Businesses may choose to implement more equitable data practices in the corporate world as a result of regulatory or reputational concerns.

Academically, there is room for more research in this field, such as looking at real user-website agreements or the economics of data exchanges. One may anticipate the emergence of a hybrid doctrine over time, in which data may be taken into account provided specific requirements (such as informed permission and privacy compliance) are fulfilled. As some have suggested with data trusts or marketplaces, a future scenario might entail controlled markets for personal data.

Ultimately, the law will need to balance innovation with individual rights. "Dignity slips away if ignored, so fairness must tag along" in online contracts, as the Lawscape conclusion warns . The concept of valid consideration may bend, but it need not break: by updating rules to the digital context, India can harness the benefits of the digital economy while upholding justice.

CONCLUSION

The notion of consideration in Indian contract law has been examined in relation to the data-driven economy of today. In addition to being technologically neutral, traditional contract principles (Section 2(d)) may be sufficiently expansive to cover non-monetary transactions [1]. Modern digital platforms, however, make things more difficult because users frequently divulge important personal information without explicit consent.

[15] The Privacy Conundrum: An Empirical Examination of Barriers to Privacy Among Indian Social Media Users – The Philosophy and Law of Information Regulation in India
https://publications.clpr.org.in/the-philosophy-and-law-of-information-regulation-in-india/chapter/1/

We discovered that since data exchange for a service is an act carried out at the promisor's request, it might theoretically satisfy the technical conditions of consideration [1]. Electronic contracts that meet the requirements of offer, acceptance, and consideration are further validated by the Information Technology Act of 2000[16]. However, there are significant disclaimers. Public policy (Section 23) and privacy rights (as upheld in Puttaswamy) act as restraints. Despite having a minimal "price," contracts that violate private rights or are unethical may be null and void. Although there isn't a definite ban on valuing data, the literature also doesn't fully support it.

In conclusion, the underlying economics of "free" services can be reflected in digital contracts by using personal data as consideration. However, improvements are required for such contracts to be just and enforceable. Statutory and judicial clarity should protect consent and fundamental rights while simultaneously recognizing the economic value of data. By doing this, the fundamental idea of reciprocity will be upheld and Indian contract law will continue to be strong and applicable in the digital era.

[16] Signing the Future: How E-Contracts Are Redefining Global and Indian Contract Law. https://www.vintagelegalvl.com/post/signing-the-future-how-e-contracts-are-redefining-global-and-indian-contract-law